Technical University of Munich

Thesis B.Sc.

Thesis M.Sc.

IDP, Guided Research

Decentral Trust Infrastructure

Motivation

Current research on distributed trusted systems is typically focused on blockchain technology. The Hyperledger Fabric framework [1] is a prominent example. In general, blockchains provide two basic services: (1) fault tolerant execution of transactions and (2) transparent append-only logging of transactions. To achieve these properties, blockchains incorporate several concepts (chaincode, consensus, permissions, ...). Therefore, these frameworks are often hard to understand, configure and maintain.

Our approach to transparency is different. We want to build an infrastructure which has similarities to the web of trust. In the web of trust, users verify the correctness of the binding of a public key to an other user's identity. In our approach, we want lightweight logs based on Merkle trees to verify the current status of other logs. This creates a distributed web of logs that enables a verifiable append-only behaviour and transitive trust to enable use cases that require transparency but also privacy.

Your task is to design such a decentralized infrastructure. In this infrastructure, an entity can join by operating an append-only log (merkle tree). In this log, the entity saves every trade it commits including a reference to the entry of the trade partner, which also operates such a log. This enables partners to mutually verify the state of the log at certain times. By applying the trust transitively, use cases such as supply chains and banking are conceivable.

Your Tasks

- Understand merkle trees
- Determine the requirements for a decentralised system based on append-only logs (merkle tree)
- Design a decentralised trust infrastructure
- Explore possible use cases such as supply chains and banking
- Evaluate its limitations

References

[1] Androulaki, Elli, et al. ”Hyperledger fabric: a distributed operating system for permissioned blockchains.” Proceedings of the Thirteenth EuroSys Conference. 2018.

[2] Laurie, Ben. ”Certificate transparency.” Communications of the ACM 57.10 (2014): 40-46.

Contact

Johannes Schleger schleger@net.in.tum.de
Dr. Holger Kinkelin kinkelin@net.in.tum.de
Richard von Seck seck@net.in.tum.de